

AMENDMENTS TO THE CLAIMS

Claims 1-23 (Canceled)

Claim 24 (Currently Amended): A method performed by a machine comprising:

- receiving a user password;
- receiving a name of an independent software application ~~that requires~~ a password for a user to use the software application;
- determining a ~~correct~~ specific salt value ~~for~~ associated with the software application;
- computing an software application dependent password for a user, wherein the software application dependent password depends on the user password and the salt value for the software application; and
- returning the software application dependent password to the software application.

Claim 25 (Currently Amended): The method of claim 24, wherein the computing of the software application dependent password depends on a user name.

Claim 26 (Currently Amended): The method of claim 25, wherein the computation of the software application dependent password further includes hashing the user name, the user password, and the salt value for the software application.

Claim 27 (Currently Amended): The method of claim 25, further comprising ~~retrieving~~ generating an old password if the old password is required.

Claim 28 (Currently Amended): The method of claim 25, wherein a strong password is used to generate a plurality of software application passwords.

Claim 29 (Currently Amended): The method of claim 24, wherein the salt value is unique for a user and an software application.

Claim 30 (Currently Amended): A method performed by a machine comprising:

generating a hash from a particular salt value associated with a specific software application and input data;
generating a password from the hash; and
returning the password to ~~an~~ the software application ~~application~~ to gain entry to the software application.

Claim 31 (Previously Presented): The method of claim 30, further comprising:
receiving the input data;
determining if the salt value exists;
generating the salt value and storing the salt value in a table entry if the salt value does not exist; and
retrieving the salt value from the table entry if the salt value exists.

Claim 32 (Previously Presented): The method of claim 30, wherein the input data comprises a user identification and a strong password.

Claim 33 (Currently Amended): The method of claim 32, wherein the input data further comprises an software application identification.

Claim 34 (Previously Presented): The method of claim 32, further comprising
determining if a new strong password is required; and
retrieving the new strong password if the new strong password is required.

Claim 35 (Currently Amended): The method of claim 32, wherein the strong password is used to generate a plurality of software application passwords.

Claim 36 (Previously Presented): The method of claim 30, wherein the salt value is one of predetermined and generated by a random number generator.

Claim 37 (Currently Amended): The method of claim 30, wherein the salt value and the software application are associated in the table entry.

Claim 38 (Currently Amended): The method of claim 30, wherein the software application is run on one of a local computer system and a networked computer system.

Claim 39 (Previously Presented): The method of claim 30, wherein one of a secure hash algorithm (SHA-1) and a message digest (MD5) algorithm are used to generate the hash.

Claim 40 (Previously Presented): The method of claim 30, wherein the generated password is temporarily stored in a memory for a predetermined time period.

Claim 41 (Previously Presented): The method of claim 40, wherein the predetermined time period is based on platform activity.

Claim 42 (Previously Presented): The method of claim 41, wherein the platform is one of a local computer system and a networked computer system.

Claim 43 (Currently Amended): A program storage device readable by a machine comprising instructions that cause the machine to:

generate a hash from a particular salt value associated with a specific software application and input data;

generate a password from the hash; and

return the password to ~~an~~ the software application to gain entry to the software application.

Claim 44 (Previously Presented): The program storage device of claim 43, further comprises instructions that cause the machine to:

receive input data;

determine if a salt value exists;

generate a salt value and store the salt value in a table entry if the salt value does not exist; and

retrieve the salt value from the table entry if the salt value exists;

Claim 45 (Previously Presented): The program storage device of claim 43, wherein the input data comprises a user identification and a strong password.

Claim 46 (Currently Amended): The program storage device of claim 45, wherein the input data further comprises ~~an~~ software application identification.

Claim 47 (Previously Presented): The program storage device of claim 43, further comprises instructions that cause the machine to:
determine if a new strong password is required; and
retrieve the new strong password if the new strong password is required.

Claim 48 (Currently Amended): The program storage device of claim 47, wherein the strong password is used by the machine to generate a plurality of software application passwords.

Claim 49 (Previously Presented): The program storage device of claim 43, wherein the salt value is one of predetermined and generated by a random number generator.

Claim 50 (Currently Amended): The program storage device of claim 43, wherein the salt value and the software application are associated in the table entry.

Claim 51 (Previously Presented): The program storage device of claim 43, wherein one of a secure hash algorithm (SHA-1) and a message digest (MD5) algorithm are used in instructions to cause the machine to generate the hash.

Claim 52 (Previously Presented): The program storage device of claim 43, wherein the generated password is temporarily stored in a memory for a predetermined time period.

Claim 53 (Previously Presented): The program storage device of claim 52, wherein the predetermined time period is based on platform activity.

Claim 54 (Previously Presented): The program storage device of claim 52, wherein the platform is one of a local computer system and a networked computer system.